U.S. Patent Application No.: 09/865,667
Attorney Docket No.: 57983.000041
Client Reference No.: 13291ROUS01U

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	
Michael G. LEE et al.	Group Art Unit: 2134
Appln. No.: 09/865,667	Examiner: Andrew L. Nalven
Filed: May 29, 2001	Confirmation No.: 4126
For: METHOD AND APPARATUS FOR SECURELY TRANSMITTING ENCRYPTED DATA THROUGH A FIREWALL AND FOR MONITORING USER TRAFFIC	Customer No.: 21967

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL

Sir:

Submitted herewith is a Reply Brief for the above-identified patent application.

[X] No additional fee is required.

[ ] Also attached: Return Post Card

[X] The fee is calculated as shown below:

	PRESENT # OF CLAIMS	HIGHEST # PREVIOUSLY PAID FOR	EXTRA CLAIMS	RATE	FEE
Total Claims	12	20		x $50 =	$.00
Independent Claims	6	6		x $200 =	$.00
		Multiple Dependent Claims Fee			$.00
		Subtotal			$.00
		Subtract ½ if Small Entity			$.00
		TOTAL FEE DUE			$.00

[ ] Please charge Deposit Account No. 50-0206 in the amount of $.00 for the above-indicated fees. A duplicate copy of this transmittal is submitted herewith.

[X] The Commissioner is hereby authorized to charge any shortage in fees under 37 CFR 1.16 and 1.17 associated with the filing of this communication, or credit any overpayment, to Deposit Account No. 50-0206. This authorization does not include any issue fees under 37 CFR 1.18. A duplicate copy of this transmittal is submitted herewith.

Respectfully submitted,

Hunton & Williams LLP

By: _____
Thomas E. Anderson
Registration No. 37,063

TEA/vrp

Hunton & Williams LLP
1900 K Street, N.W.
Washington, D.C. 20006-1109
Telephone: (202) 955-1500
Facsimile: (202) 778-2201
Date: April 13, 2007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	
Michael G. LEE et al.	Group Art Unit: 2134
Appln. No.: 09/865,667	Examiner: Andrew L. Nalven
Filed: May 29, 2001	Confirmation No.: 4126
For: METHOD AND APPARATUS FOR SECURELY TRANSMITTING ENCRYPTED DATA THROUGH A FIREWALL AND FOR MONITORING USER TRAFFIC	Customer No.: 21967

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

Sir:

This Reply Brief is submitted in response to the Examiner's Answer dated February 13, 2007.

ARGUMENT

The Examiner's Answer dated February 13, 2007 has been received and carefully considered. The rejections of claims 1, 2, 4-8, and 10-12 under 35 U.S.C. § 102(e) as being anticipated by Perlman et al. (U.S. Patent No. 6,546,486) and claims 3 and 9 under 35 U.S.C. § 103(a) as being unpatentable over Perlman in view of Ylonen et al. (U.S. Patent No. 6,438,612) still stand.

In the Examiner's Answer, the Examiner asserts that Perlman et al. discloses the claimed invention. Appellants respectfully disagree. Specifically, Appellants respectfully submit that Perlman et al. fails to teach, or even suggest, the steps of detecting an exchange of a first encryption key between a host device and a remote device, and exchanging a second encryption key with the host device, as claimed.

The Examiner asserts that the claimed "second key" is disclosed by the "second exchange" of the message key. The Examiner relies on col. 6, lines 4-13 of Perlman et al. to allegedly disclose detecting an exchange of a first encryption key between a host device and a remote device, and exchanging a second encryption key with the host device. *See* Examiner's Answer dated February 13, 2007 at p. 6. However, Appellants respectfully disagree. The claimed "second key" is not the same as the "second exchange" of the message key. In fact, the cited portion only refers to one key - message key 204. This is clearly distinguishable from detecting an exchange of a *first encryption key* between a host device and a remote device, and exchanging a *second encryption key* with the host device.

Furthermore, even assuming, for the sake of argument, that Perlman et al. discloses a "second key," which the Examiner previously equated with the firewall public key of Perlman et

al. (see Office Action dated February 28, 2006 at p. 2), then Perlman et al. still fails to disclose detecting an exchange of a first encryption key between a host device and a remote device. As disclosed in Perlman et al., Key 204 (i.e., the alleged claimed "first key") is not detected but rather is *passed* to destination 110 for decryption at the destination. Therefore, even if the "public key" disclosed by Perlman et al. is considered to be the claimed "second key," then Perlman et al. fails to disclose the claimed features of the "first key."

The Examiner also asserts, in the Examiner's Answer dated February 13, 2007, that Perlman et al. teaches "exchanging a second encryption key with the host device (Perlman, column 6, lines 10-14, "secure manner", column 5, line[] 65 - column 6 line 4)." *See* Examiner's Answer at p. 6. However, as discussed above, it appears that Examiner again confuses the "second key" with the alleged "second exchange" of the first key. Indeed, that Examiner goes to great length to discuss how the alleged "second key" is exchanged "once the exchange of the first key is detected" in a "secure manner." *See* Examiner's Answer at p. 6. However, Appellants respectfully submit Perlman et al., at best, discloses using one message key 204 (the alleged "first key") in several steps/negotiations. In fact, the Examiner acknowledges that "once the exchange of the first message key occurs between

the source and the destination then ***the*** message key [referring to the first message key] is exchanged between the source or destination and the firewall in a secure manner." *See* Examiner's Answer at p. 6 (emphasis added).

As a result, the alleged "second exchange" does not suffice to teach or suggest that a "second key" is detected or exchanged, as claimed.

In view of the foregoing, it is respectfully submitted that Perlman et al. fails to teach, or even suggest, the claimed invention as set forth in claim 1. Thus, is it further respectfully submitted that claim 1 is allowable over Perlman et al.

Claim 2 is dependent upon independent claim 1. Thus, since independent claim 1 should be allowable as discussed above, claim 2 should also be allowable at least by virtue of its dependency on independent claim 1. Moreover, claim 2 recites additional features which are not disclosed, or even suggested, by Perlman et al.. For example, claim 2 recites not allowing encrypted data to pass when it is determined that the first encryption key is not received. Perlman et al. fails to disclose, or even suggest, such claimed features.

Regarding claims 4, 5, 7, 10, and 11, these claims recite subject matter related to claim 1. Thus, the arguments set

forth above with respect to claim 1 are equally applicable to claims 4, 5, 7, 10, and 11. Accordingly, is it respectfully submitted that claims 4, 5, 7, 10, and 11 are allowable over Perlman et al. for the same reasons as set forth above with respect to claim 1.

Claims 6, 8, and 12 are dependent upon independent claims 5, 7, and 11, respectively. Thus, since independent claims 5, 7, and 11 should be allowable as discussed above, claims 6, 8, and 12 should also be allowable at least by virtue of their dependency on independent claims 5, 7, and 11. Moreover, these claims recite additional features which are not disclosed, or even suggested, by Perlman et al.. For example, claim 8 recites an encrypted data blocker for not allowing encrypted data to pass when it is determined that the first encryption key is not received. Perlman et al. fails to disclose, or even suggest, such claimed features.

In view of the foregoing, it is respectfully submitted that Perlman et al. fails to disclose, or even suggest, the elements of claims 1, 2, 4-8, and 10-12. Accordingly, it is respectfully submitted that claims 1, 2, 4-8, and 10-12 of the present application are not anticipated by Perlman et al., and thus the Examiner has failed in his duty to establish at least a prima facie case of anticipation against claims 1, 2, 4-8, and 10-12

of the present application. Therefore, it is respectfully requested that the anticipation rejection of claims 1, 2, 4-8, and 10-12 be withdrawn.

With regard to claims 3 and 9, it is respectfully submitted that the obviousness rejection of these claims has become moot in view of the deficiencies of the primary reference Perlman et al. as discussed above with respect to independent claims 1 and 7, respectively. That is, claims 3 and 9 are dependent upon independent claims 1 and 7, respectively, and thus inherently incorporate all of the limitations of independent claims 1 and 7, respectively.

Moreover, the secondary reference Ylonen et al. fails to disclose, or even suggest, the deficiencies of the primary reference Perlman et al. as discussed above with respect to independent claims 1 and 7. Indeed, the Examiner does not even assert such. Thus, the combination of the secondary reference Ylonen et al. with the primary reference Perlman et al. also fails to disclose, or even suggest, the deficiencies of the primary reference Perlman et al. as discussed above with respect to independent claims 1 and 7. Accordingly, claims 3 and 9 should be allowable over the combination of the secondary reference Ylonen et al. with the primary reference Perlman et al. at least by virtue of their dependency on independent claims

1 and 7. Moreover, claims 3 and 9 recite additional features which are not disclosed, or even suggested, by the cited references taken either alone or in combination. For example, claims 3 and 9 recite detecting an exchange of a first encryption key by monitoring Internet Key Exchange (IKE) protocol data traffic to determine whether the first encryption key is exchanged. Perlman et al. and Ylonen et al., either alone or in combination, fail to disclose, or even suggest, such claimed features, particularly when viewed in combination with the features of independent claims 1 and 7.

In the Examiner's Answer, however, the Examiner asserts that Ylonen et al. discloses the "use of the IKE protocol to exchange keys (Ylonen, column 5 line 55 - column 6 line 5)." *See* Examiner's Answer at p. 8. However, Appellants respectfully disagree.

The Examiner asserts that modifying Perlman et al. to include the alleged use of the IKE protocol feature of Ylonen et al. would have been obvious because the modification because "it offers the advantage of using a key management scheme that provides authentication between source and destination while adhering to an industry standard method of key exchange (Ylonen, column 4 lines 39-59)." *See* Examiner's Answer at p. 8. However, such a statement represents classic **impermissible**

hindsight. The Examiner fails to provide any ***evidence*** as to why one of ordinary skill in the art would choose to implement the alleged IKE protocol element in the way claimed. Apparently, the Examiner's statement that it would offer "the advantage of using a key management scheme that provides authentication between source and destination while adhering to an industry standard method of key exchange" is wholly unsupported. In fact, nowhere in Ylonen et al. is this alleged statement of motivation even mentioned.

Furthermore, the Examiner fails to set forth an explanation as to why one of ordinary skill in the art would have been motivated to use alleged IKE protocol element as in Ylonen et al. with a scheme as in Perlman et al., or if one did, how that would work. In other words, the Examiner provides no explanation as to how Ylonen et al.'s system, which is directed to secure tunneling of data between virtual routers, may be combined with the end-to-end encryption system of Perlman et al. to form the step of detecting an exchange of a first encryption key by "monitoring Internet Key Exchange (IKE) protocol data traffic to determine whether the first encryption key is exchanged," as expressly recited in claims 3 and 9. As a result, there is no suggestion that Perlman et al. or Ylonen et al. could be modified to permit monitoring Internet Key Exchange

(IKE) protocol data traffic to determine whether the first encryption key is exchanged.

In view of the foregoing, it is respectfully submitted that the combination of the primary reference Perlman et al. with the secondary reference Ylonen et al. fails to disclose, or even suggest, the elements of claims 3 and 9. Accordingly, it is respectfully submitted that claims 3 and 9 of the present application are not unpatentable over the combination of the primary reference Perlman et al. with the secondary reference Ylonen et al., and thus the Examiner has failed in his duty to establish at least a prima facie case of obviousness against claims 3 and 9 of the present application. Therefore, it is respectfully requested that the obviousness rejection of claims 3 and 9 be withdrawn.

CONCLUSION

In view of the foregoing, it is respectfully submitted that the Examiner has failed to establish a prima facie case of anticipation against the appealed claims. Thus, it is respectfully submitted that the final rejection of claims 1-6, 19, and 20 is improper and the reversal of same is clearly in order and respectfully requested.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-0206, and please credit any excess fees to such deposit account.

Respectfully submitted,

Hunton & Williams LLP

By: _____
Thomas E. Anderson
Registration No. 37,063

TEA/vrp

Hunton & Williams LLP
1900 K Street, N.W.
Washington, D.C. 20006-1109
Telephone: (202) 955-1500
Facsimile: (202) 778-2201

Date: April 13, 2007